IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

SOPHIA HARTLEY, individually and on behalf of all others similarly situated, Plaintiff, v. UNIVERSITY OF CHICAGO MEDICAL CENTER, Defendant.	Case No. 22-cv-5891

THIRD AMENDED CLASS ACTION COMPLAINT

Sophia Hartley ("Plaintiff"), individually and for all others similarly-situated, by and through their undersigned counsel, bring this action against University of Chicago Medical Center ("UCMC" or "Defendant"), alleging as follows:

NATURE OF THE ACTION

1. Plaintiff brings this action for herself and thousands of other patients whose medical privacy has been violated by UCMC's use of Meta Platform Inc.'s ("Meta") tracking and collection tools, including the Meta Pixel, Meta SDK, Meta Conversions API, customer list uploads, social plug-ins, the Meta Graph API, server-to-server transmissions, and all similar collection tools (collectively, "Meta Collection Tools"). The Meta Collection Tools allow UCMC to intercept individually-identifiable health information from UCMC's website and monetize this information for its own financial gain.

2. Meta operates the world's largest social media company. Meta's revenue is derived almost entirely from selling targeted advertising. Meta's "Health" division is dedicated to marketing to and servicing Meta's healthcare "Partners." Meta defines its "Partners" to include

"businesses" that use Meta's products, including the Meta Pixel or Meta Audience Network tools "to advertise, market, or support their products and services."

3. Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.

4. Plaintiff is a UCMC patient who alleges that UCMC installed the Meta Collection Tools on its public website www.uchicagomedicine.org, (UCMC's "Website") to share her confidential health information with Meta for financial gain in violation of federal and state laws, and despite Defendant's express promise that it: "will not disclose [its patients'] health information for purposes other than your treatment without your prior written consent."[1]

5. When a patient uses UCMC's Website where Meta Collection Tools are present, the Meta Collection Tools transmit the content of their communications to Meta, including, but not limited to: (1) signing-up for a patient portal; (2) signing-in or -out of a patient portal; (3) taking actions inside a patient portal; (4) making, scheduling, or participating in appointments; (5) exchanging communications relating to doctors, treatments, payment information, health insurance information, prescription drugs, prescriptions, side effects, conditions, diagnoses, prognoses, or symptoms of health conditions; (6) conducting a search on UCMC's Website; and (7) other information that qualifies as "protected health information" under federal and state laws.

6. Meta Collection Tools also collect and transmit information from UCMC that identifies a Facebook user's status as a patient and other health information that is protected by federal and state law. This occurs through tools that Meta encourages its healthcare Partners to

[1] Notice of Privacy Policies, *available at* https://wellness.uchicago.edu/about/notices/

use to upload customer lists to Meta for use in its advertising systems. In the case of UCMC, a customer list is a patient list.

7. The information transmitted from UCMC's Website to Meta always includes information sufficient to uniquely identify a patient under federal law (such as IP address information, device identifiers, and advertising identifiers that Meta associates with a patient's Meta account), and may also include a patient's demographic information, email address, phone number, computer ID address, or contact information entered as emergency contacts or for advanced care planning, along with information like appointment type and date, a selected physician, button and menu selections, the content of buttons clicked and typed into text boxes, and information about the substance, purport, and meaning of patient requests for information from UCMC under federal and state health privacy laws.

8. The transmission of this information is instantaneous, invisible, and occurs without any notice to the patient that it is occurring.

9. Meta collects the transmitted identifiable health information and uses "cookies" to match it to Facebook users, allowing UCMC to target advertisements both on and off Facebook. For example, UCMC and Meta can target ads to a person who has used a patient portal and exchanged communications about a specific condition, such as cancer.

10. Instead of taking proactive steps to verify that businesses using Meta Pixels obtain the required consent, Meta uses an "honor system" under which Meta assumes these businesses have "provided robust and sufficient prominent notice to users regarding the Business Tool Data collection, sharing, and usage." *See* Facebook Business Tools Terms, *https://www.facebook.com/legal/terms/businesstools*.

11. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996) and Illinois' law relating to the confidentiality of medical records, 410 ILCS 50 *et seq.*, both prohibit healthcare providers from sharing health care information, medical records, and related information with third parties except as needed for a patient's treatment, payment, or with their consent. Importantly, these laws give patients a reasonable expectation of privacy in communications with healthcare providers relating to their medical conditions and treatment, because this information may not be disclosed outside the healthcare setting without notice and consent.

12. The United States Department of Health and Human Services ("HHS") recently confirmed that HIPAA and its regulations prohibit the transmittal of individually identifiable health information by tracking technology like the Meta Pixel without the patient's authorization and other protections like a business associate agreement with the recipient of patient data.[2]

13. Meta's Terms of Service, Data Policy, and Cookies Policy neither inform Facebook users that Meta may acquire their health information when they interact with healthcare providers' websites and applications, nor obtain their consent for any such acquisitions.

14. UCMC's interception, dissemination, and use of individually-identifiable health information not only violates federal and state law but also harms patients by intruding upon their privacy; erodes the confidential nature of the provider-patient relationship; and takes patients' property and property rights without compensation and ignores their right to control the dissemination of their health information to third parties. In addition, UCMC has been unjustly

[2] *See* Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.*

enriched by its misconduct, obtaining unearned revenues derived from its unauthorized disclosure of patient information.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over the claims that arise under the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq*.

16. This Court also has subject-matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), which, under the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(d), 1453 and 1711-15 ("CAFA"), expressly provides federal courts with jurisdiction over any class action in which: the proposed class includes at least 100 members; any member of the class is a citizen of a state and any defendant is a citizen or subject of a foreign state; and the amount in controversy exceeds $5,000,000.00, exclusive of interest and costs.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant does business in, and is subject to, personal jurisdiction in this District. Venue is also proper in this District, because a substantial part of the events or omissions giving rise to the claim occurred in, and emanated from, this District.

MATERIAL FACTS

Meta's Collection Tools Redirect Patients' Data From UCMC's Website To Use For Ad Targeting

18. Meta maintains profiles of its Facebook users that include the users' real names, locations, email addresses, friends, "likes," and communications.

19. Meta associates this information with personal identifiers, including IP addresses, cookies, device identifiers, and advertising ID identifiers.

20. Meta also tracks non-users across the web through its widespread Internet marketing products and source code, including the Meta Pixel.

21. Meta's revenue is derived almost entirely from selling targeted advertising, which includes, but is not limited to, targeted advertising to Meta properties and to all Internet users on non-Meta sites and apps.

22. Meta's Business division provides advertising services and tools to web developers, including the Meta Collection Tools. Meta's Business division and its advertising services and tools are focused on trade and commerce.

23. The Meta Pixel is a free and publicly available "piece of code" that third-party web developers can install on their website to "measure, optimize and build audiences for … ad campaigns."[3]

24. Meta describes the Pixel as "a snippet of Javascript code" that "relies on Facebook cookies, which enable [Facebook] to match … website visitors to their respective Facebook User accounts.[4]

25. Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers the Pixel "can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart."[5]

26. Meta tells advertisers that the Meta Pixel will improve their Facebook advertising, including by allowing them to:

a. "measure cross-device conversions" and "understand how your cross-device ads help influence conversion.";

b. "optimize the delivery of your ads" and "[e]nsure your ads reach the people most likely to take action;" and

c. "create Custom Audiences from website visitors" and create "[d]ynamic ads [to] help you automatically show website

[3] Meta, Meta Pixel (2023), *https://www.facebook.com/business/tools/meta-pixel.*
[4] Meta for Developers, Meta Pixel (2023), *https://developers.facebook.com/docs/meta-pixel/.*
[5] Meta, Meta Pixel (2023), *https://www.facebook.com/business/tools/meta-pixel.*

> visitors the products they viewed on your website—or related ones."[6]

27. Meta explains that the Pixel "log[s] when someone takes an action on your website" such as "adding an item to their shopping cart or making a purchase," and the user's subsequent action:

> Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Meta Pixel receives these actions, or events, which you can view on your Meta Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. You'll also have options to reach those customers again through future Facebook ads.

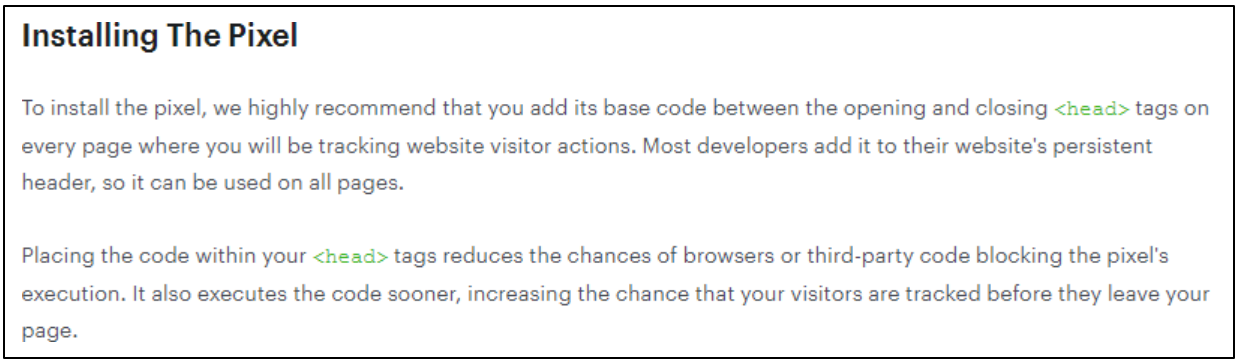
28. The Meta Pixel is customizable. Web developers can choose the actions the Pixel will track and measure.

29. Meta advises web developers to place the Pixel early in the source code for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website:[7]

---

[6] *Id.*

[7] Meta For Developers, Get Started (2023), *https://developers.facebook.com/docs/meta- pixel/get-started.*



Installing The Pixel

To install the pixel, we highly recommend that you add its base code between the opening and closing <head> tags on every page where you will be tracking website visitor actions. Most developers add it to their website's persistent header, so it can be used on all pages.

Placing the code within your <head> tags reduces the chances of browsers or third-party code blocking the pixel's execution. It also executes the code sooner, increasing the chance that your visitors are tracked before they leave your page.

30. Meta also provides advertisers with step-by-step instructions for setting up and installing the Meta Pixel on their website, so that companies can add the Meta Pixel to their website without a developer.[8]

31. If a healthcare provider, such as UCMC, installs the Meta Pixel code as Meta recommends, patients' actions on the provider's website are contemporaneously redirected to Meta. When a patient clicks a button to register for, or logs into or out of, a "secure" patient portal, Meta's source code commands the patient's computing device to send the content of the patient's communication to Meta while the patient is communicating with her healthcare provider. In other words, by design, Meta receives the content of a patient's portal log in communication immediately when the patient clicks the log-in button—even before the healthcare provider receives it.

32. Thus, the Meta "pixel allows Facebook to be a silent third-party watching whatever you're doing."[9]

33. UCMC discloses the content of the communication to Meta while the patient is exchanging the communication with UCMC's Website.

---

[8] Meta, Meta Pixel (2023), *https://www.facebook.com/business/tools/meta-pixel.*

[9] Jefferson Graham, *Facebook spies on us but not by recording our calls. Here's how the social network knows everything*, USA Today (March 4, 2020 4:52 am), *https://www.usatoday.com/story/tech/2020/03/04/facebook-not-recording-our-calls-but-has-other-ways-snoop/4795519002/#.*

Meta Uses Identifiers To Match The Health Information It Collects With Facebook Users

34. Meta uses cookies to identify patients, including cookies named c_user, datr, fr, and _fbp.

35. The c_user cookie identifies Facebook users. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one – and only one – unique c_user cookie. Meta uses the c_user cookie to record user activities and communications.

36. An unskilled computer user can obtain the c_user cookie value for any Facebook user by (1) going to the user's Facebook page, (2) right-clicking with their mouse, (3) selecting "View page source," (4) executing a control-f function for "UserID," and (5) copying the number value that appears after "UserID" in the page source code of the Facebook user's page.

37. Following these directions makes it possible to discover that the Facebook UserID assigned to Mark Zuckerberg is 4. By typing *www.facebook.com/4* into a browser and hitting enter, a browser directs to Mr. Zuckerberg's page at *www.facebook.com/zuck*.

38. The Meta datr cookie identifies the web browser the patient is using. It is an identifier unique to each patient's specific web browser, so is another way Meta can identify Facebook users.

39. Meta keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Meta by using the Facebook "Download Your Information" tool.

40. The Meta fr cookie is an encrypted combination of the c_user and datr cookies.[10]

41. The c_user, datar, and fr cookies are traditional third-party cookies, meaning they are cookies associated with a party other than the entity with which a person is communicating at the time. In the case of UCMC, they are third-party cookies because Meta is a third-party to the communication between a patient and their healthcare provider.

42. The Meta _fbp cookie is a Facebook identifier that is set by Facebook source code and associated with the healthcare provider using the Meta Pixel.

43. The letters fbp are an acronym for Facebook Pixel.

44. The _fbp (or Facebook Pixel) cookie is also a third-party cookie in that it is also a cookie associated with Meta that is used by Meta to associate information about a person and their communications with non-Meta entities while the person is on a non-Meta website or application.

45. Meta disguises the _fbp cookie as a first-party cookie even though it is Meta's cookie on non-Meta websites.

46. By disguising the _fbp cookie as a first-party cookie for a healthcare provider rather than a third-party cookie associated with Facebook, Meta ensures that the _fbp cookie is placed on the computing device of patients who seek to access the patient portal.

47. Healthcare providers with a patient portal require patients to enable first-party cookies to gain access to their patient records through the portal.

48. The purpose of these portal-associated first-party cookies is security. The _fbp cookie is then used as a unique identifier for that patient by Meta. If a patient takes an action to

[10] *See* Gunes Acar, *et al.*, Facebook Tracking Through Social Plug-ins: Technical Report Prepared for the Belgian Privacy Commission (Mar. 27, 2015), *https://securehomes.esat.kuleuven.be/~ gacar/fb_tracking/fb_pluginsv1.0.pdf.*

delete or clear third-party cookies from their device, the _fbp cookie is not impacted – even though it is a Meta cookie – again, because Meta has disguised it as a first-party cookie.

49. Meta also uses IP address and user-agent information to match the health information it collects from Meta healthcare Partners with Facebook users.

Meta Encourages Healthcare Partners, Including UCMC, To Upload Patient Lists For Ad Targeting

50. Meta offers an ad targeting option called "Custom Audiences." When a patient takes an action on a Meta healthcare Partner's website embedded with the Pixel, the Pixel will be triggered to send Meta "Event" data that Meta matches to its users. A web developer can then create a "Custom Audience" based on Events to target ads to those patients. The Pixel can then be used to measure the effectiveness of an advertising campaign.[11]

51. Meta also allows Meta healthcare Partners to create a Custom Audience by uploading a patient list to Meta. As Meta describes it:[12]

> A Custom Audience made from a customer list is a type of audience you can create to connect with people who have already shown an interest in your business or product. It's made of information - called "identifiers" - you've collected about your customers (such as email, phone number and address) and provided to Meta. Prior to use, Meta hashes this information.
>
> Then, we use a process called matching to match the hashed information with Meta technologies profiles so that you can advertise to your customers on Facebook, Instagram and Meta Audience Network. The more information you can provide, the better the match rate (which means our ability to make the matches). Meta doesn't learn any new identifying information about your customers.

[11] Meta Business Help Center, *About Customer List Custom Audiences* (2023), *https://www.facebook.com/business/help/341425252616329?id=2469097953376494*; *see also,* Meta Blueprint, Connect your data with the Meta Pixel and Conversion API (2023), *https://www.facebookblueprint.com/student/activity/212738?fbclid=IwAR3HPO1d_fnzRCUAhKGYsLqNA-VcLTMr3G_hxxFr3GZC_uFUcymuZopeNVw#/page/5fc6e67d4a46d349e9dff7fa*

[12] Meta Business Help Center, *About Customer List Custom Audiences* (2023), *https://www.facebook.com/business/help/341425252616329?id=2469097953376494*.

52. Meta provides detailed instructions for healthcare Partners to send their patients' individually-identifiable information to Meta through the customer list upload. For example:

> **Prepare your customer list in advance.** To make a Custom Audience from a customer list, you provide us with information about your existing customers and we match this information with Meta profiles. The information on a customer list is known as an "identifier" (such as email, phone number, address) and we use it to help you find the audiences you want your ads to reach.
>
> Your customer list can either be a CSV or TXT file that includes these identifiers. To get the best match rates, use as many identifiers as possible while following our formatting guidelines. You can hover over the identifiers to display the formatting rules and the correct column header. For example, **first name** would appear as **fn** as a column header in your list.
>
> Alternatively, we have a file template you can download to help our system map to your identifiers more easily. (You can upload from Mailchimp as well.)

53. Meta healthcare Partners can then use the Custom Audiences derived from their patient list with the Pixel and Pixel Events for Meta marketing campaigns and to measure the success of those campaigns.

UCMC Sends A Broad Spectrum Of Identifiable Health Information To Meta Through The Meta Collection Tools

54. The information UCMC sends to Meta from its use of the Meta Collection Tools includes, but is not limited to, the following:

a. when a patient clicks to register for a patient portal;

b. information that a patient types into registration forms;

c. when a patient clicks to log in to a patient portal;

d. when a patient clicks to log out of a patient portal;

e. when a patient sets up or schedules an appointment;

f. information that a patient types into an appointment form;

g. when a patient clicks a button to call the provider from a mobile device directly from the provider's website;

h. descriptive URLs that describe the categories of the website, categories that describe the current section of the website, and the referrer URL that caused navigation to the current page;

i. the communications a patient exchanges through UCMC's Website by clicking and viewing webpages, including communications about providers and specialists, conditions, and treatments, along with the timing of those communications, including whether they are made while a patient is still logged in to a patient portal or around the same time that the patient has scheduled an appointment, called the medical provider, or logged in or out of the patient portal; and

j. the same or substantially similar communications that patients exchange with health insurance companies, pharmacies, and prescription drug companies.

55. UCMC's conduct constitutes an egregious breach of social norms as demonstrated by public polling that shows: "[n]inety-seven percent of Americans believe that doctors, hospitals, labs, and health technology systems should not be allowed to share or sell their sensitive health information without consent."[13]

Plaintiff's Allegations Include UCMC's Use Of Meta's Other Collection Tools And Both Website And Applications

56. Defendant's use of Meta's Collection Tools on its Website caused the interception and disclosure to Meta of thousands of UCMC's patients' individually identifiable health information.

57. UCMC collects patients' health information on its websites and applications using the same technology, namely Javascript source code that commands a patient's browser or application to re-direct Event Data through the HTTPS protocol to Meta at a Meta "endpoint," *i.e.*, a URL at a domain controlled by Meta that exists for the purpose of acquiring such information.

[13] *Poll: Huge majorities want control over health info,* Healthcare Finance (Nov. 10, 2020), *https://www.healthcarefinancenews.com/news/poll-huge-majorities-want-control-over-health-info.*

58. UCMC also uses the Meta Pixel in mobile "hybrid" applications. A hybrid application is created using identical source code and language to display a web-property on an application or through a website on a browser application. The benefit of a hybrid application is that identical source code can be used across all web-properties – *i.e.*, a website, an Android application, and an iOS application. Meta provides source code for "hybrid apps" and states that its code "convert[s] Facebook Pixel events into App events."

59. Meta combines health information on specific persons across different devices and different Meta endpoints. Meta can—and does—associate health information with individual patients gathered across different devices and across different healthcare provider web properties, including both websites and applications.

60. Meta's "Consolidated Container" for Event Data – the Meta Conversions API – "enables advertisers to send web, app, and physical store events to Meta through a single endpoint rather than across multiple sources."[14] This consolidation will "simplify an advertiser's tech stack and create a more comprehensive view within Meta Events Manager by using data sets." *Id.* In addition, "App Events" can be "associated with a dataset" through which Meta "connects… event data from web, app, and store event sources to the conversions API." *Id.* The data Meta collects "may show event data from any of these integrations…, including website, app, and offline events." *Id.* As a result, "all customer activities" can be viewed "from a single interface" in a single storage location that Meta calls a "consolidated container." *Id.*

[14] Meta for Developers, *Conversions API for App events* (2023), *https://developers.facebook.com/docs/marketing-api/conversions-api/app-events/*.

61. The Facebook SDK, specifically, "can automatically log app installs, app sessions, and in-app purchases" when deployed on a healthcare provider application.[15] The Facebook SDK can also be used to log other events that users take on an application.

62. Meta's "Graph API is the primary way to get data into and out of the Facebook platform." It is based on Meta's concept of a social graph, which is a "representation of the information on Facebook" which is "composed of nodes, edges, and fields."[16]

63. Through server-to-server transmissions, developers "can share data directly [with Meta] from [their] server, rather than through a browser."[17]

64. When a HIPAA-covered entity, like UCMC, installs the Pixel, SDK, and Conversions API on both its website and application, Meta collects Event Data from the website and the application, places it in a consolidated container, uses the comingled information, and sends the results back to the entity.

UCMC Violates Its Own Privacy Policies & Promises

65. To attract patients, enable their pursuit of medical care, foster its provision of that medical care, and support its business, the UCMC Website enable individual patients to engage in a wide array of communications concerning their individually identifiable health information.

66. With respect to patients' individually identifiable health information, UCMC recognizes and publicly acknowledges that "by law, [UCMC] must keep [its patients'] PHI private and secure."[18]

---

[15] *https://developers.facebook.com/docs/app-events/overview.*
[16] *https://developers.facebook.com/docs/graph-api/overview.*
[17] *https://developers.facebook.com/docs/marketing-api/conversions-api/guides/end-to-end-implementation/*
[18] *See https://www.uchicagomedicine.org/about-us/privacy-practices*

67. UCMC's patient portal, *www.mychart.uchospitals.edu/mychart* or "MyChart" allows its patients to communicate with UCMC with options including but not limited to "communicate with your doctor," "access your test results," and "schedule an appointment."[19]

68. With respect to patients' individually identifiable health information, UCMC states that its Student Wellness Center "uses [its patients'] health information only to provide [its patients] with medical care and counseling services, to support our own operations, and as otherwise permitted by applicable state and federal law," and that it "will not disclose [its patients'] health information for purposes other than your treatment without your prior written consent."[20]

69. Notwithstanding all these representations, UCMC designed the Meta Collection Tools to capture both the "characteristics" of individual patients' communications with the UCMC Website (*i.e.,* their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (*i.e.*, the URLs, buttons, links, pages, and tabs they click and view).

70. Notwithstanding all these representations, UCMC installed Meta's Collection Tools on its Website and, thereafter, began to automatically transmit extensive individually identifiable patient health information from everyone who visited its Website to Meta.

71. As an example, anyone who visits UCMC's public website and clicks on the "Find a Condition" tab is directed to a page, *https://www.uchicagomedicine.org/conditions-services*, and is presented with a search bar that lists approximately 599 links to pages with information on specific conditions, treatments, services, and locations, ranging from "Abdominal Aortic

[21] *https://www.businessinsider.com/facebook-changes-free-and-always-will-be-slogan-on-homepage-2019-8.*
[21] *https://www.businessinsider.com/facebook-changes-free-and-always-will-be-slogan-on-homepage-2019-8.*

Aneurysm" to "Your Child's Recovery From Surgery." Someone who clicks the "Cancer" button is directed to a page, *https://www.uchicagomedicine.org/cancer*, which includes buttons and links that provide information on specific treatment options, services, locations, and clinical trials. Selecting any of these links, like "Cancer Surgery" directs them to a new page, like *https://www.uchicagomedicine.org/cancer/types-treatments/surgery* which includes more buttons linked to specific cancer surgeries. Someone who clicks on "Radical Vaginal Trachelectomy" is directed to an additional page, *https://www.uchicagomedicine.org/cancer/types-treatments/cervical-cancer/trachelectomy*, providing information about this type of surgery, treatment options, services, providers, locations, and clinical trials, many of which have additional links and buttons.

72. The Meta Collection Tools intercept both the "characteristics" and "content" of all these communications with UCMC's Website, including individually identifiable patient health information (*i.e.*, about cancer care, cancer surgery, cancer treatment, and clinical trials) and automatically transmits this data to Meta.

73. After receiving individually identifiable health information communicated on UCMC's Website, Meta analyzes and uses this information for its own commercial purposes that include building more fulsome profiles of its users' preferences and traits, and selling more-targeted advertisements based on this information. Meta also receives an additional commercial benefit from UCMC's use of Meta's Collection Tools, namely that it provides UCMC with a greater incentive to advertise on Meta's social media platforms.

74. After receiving individually identifiable patient health information communicated on the UCMC's Website, Meta forwards this data, and its analysis of this data, to UCMC. UCMC then uses this data and analysis for its own commercial purposes that include understanding how

people use its website and determining what ads people see on its website. UCMC also receives an additional commercial benefit from using Meta's Collection Tools, namely that grants Meta access to the commercially-valuable, individually identifiable patient health information communicated on its Website.

75. Meta is not an intended recipient of the individually identifiable health information communicated by patients on UCMC's Website, nor is it an active or disclosed participant in these communications. However, Meta is the intended recipient of patient communications containing individually identifiable health information transmitted by UCMC.

76. UCMC does not notify users of its Website that it is automatically sending individually identifiable health information communicated on its Website to Meta.

77. UCMC does not notify users of its Website that individually identifiable health information they communicate on its Website is being used by Meta for commercial purposes.

78. UCMC does not notify users of its Website that it is using the individually identifiable health information they communicate on its webWebsite for commercial purposes.

79. Meta has not secured any informed consent or written permission allowing it to use individually identifiable health information communicated on UCMC's Website for commercial purposes.

80. UCMC has not secured any informed consent or written permission allowing it to share individually identifiable health information communicated on its Website with Meta.

81. UCMC has not secured any informed consent or written permission allowing it to use individually identifiable health information communicated on its Website for commercial purposes.

Meta Falsely Promises Facebook Users That It Requires Healthcare Partners To Have The Right To Share Their Data

82. Every Facebook user is legally deemed to have agreed to the Terms of Service, Data Policy/Privacy Policy, and Cookie Policy via a checkbox on the sign-up page. The Terms of Service, Data Policy/Privacy Policy, and Cookie Policy are binding on Meta and its users.

83. The Meta contract documents contain general statements that, in exchange for the use of Meta's services, Meta will generally collect information about Facebook users.

84. Meta does not charge users any money to use its services, but Meta is not "free."

85. In 2019, Meta removed language on its webpage that stated, "It's free and always will be."[21] This conduct demonstrates that using Meta is not, in fact, free. As a digital law expert has explained: "Facebook is not free nor has it ever been. Facebook's currency was and still is its users' personal data. It's never been free, though, because data is worth a lot of money." *Id.*

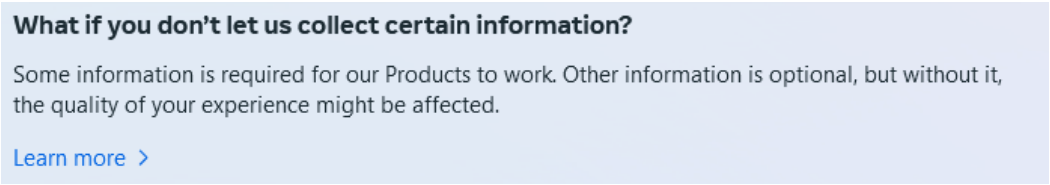
86. Rather than making users pay money out-of-pocket to use Facebook, Meta makes them pay for its services by allowing Meta to collect some types of personal data under a "data license."

87. Meta's contract states, "We collect and use your personal data in order to provide the services described above to you." It then informs users, "You can learn how we collect and use your data in our Data Policy."[22]

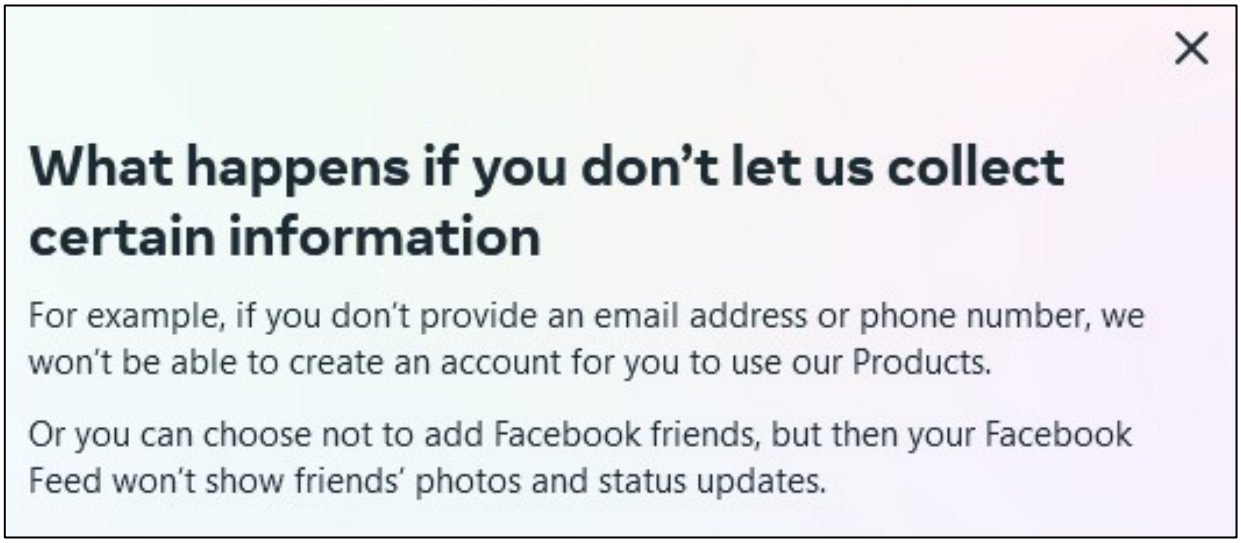
[21] *https://www.businessinsider.com/facebook-changes-free-and-always-will-be-slogan-on-homepage-2019-8.*

[22] The hyperlink to Data Policy sends users to the Meta Privacy Policy at *https://www.facebook.com/privacy/policy/?entry point=data policy redirect&entry=0.*

88. Although the Meta Data Policy makes general broad disclosures about the data it collects, the scope of Meta's "data license" is not unlimited. For example, by signing up for Meta, a Facebook user has not agreed to exchange with Meta the right for Meta to obtain their bank account information or Social Security number. Instead, the Meta Privacy Policy establishes a minimum amount of information users must provide directly to Meta to use Meta's products:



89. When a Facebook user clicks the "Learn more" hyperlink to learn what "information is required" for Facebook to work, Meta provides examples of how choosing not to share information will prevent users from creating a Facebook account or using its features:



90. Meta's Terms of Service also expressly incorporates the Meta Privacy Policy by hyperlink, stating that "Our Privacy Policy explains how we collect and use your personal data to determine some of the ads you see and provide all of the other services described" in Meta's Terms of Service.

91. The Meta Privacy Policy has a section titled "What information do we collect?" in which Meta tells users:

> Meta, we use information to provide you with a more personal, secure, and meaningful experience. But where does that information come from? The information we collect comes from a variety of sources.... *And, sometimes businesses also share information with us like your activity on their websites. They may also share experiences you have offline, like signing up for a Rewards card with your email address.* This makes it easier for them to share promotions, product information, and other ads with you through our ads consistent with the choices that you make.

(Emphasis added). *Id.*

92. The Meta Privacy Policy does not state that Meta actively solicits Facebook users' healthcare providers, health insurers, pharmacies, prescription drug companies, and other covered entities under 45 C.F.R. § 160.103 to become Meta Partners using Meta's business services.

93. The Meta Privacy Policy does not state that, in exchange for use of its Products, Meta will collect health information from a Facebook user's healthcare providers, health insurers, pharmacies, prescription drug companies, or other covered entities under 45 C.F.R § 160.103 about the Facebook user, including their communications, actions, and status as patients with those health entities.

94. In addition to not obtaining specific consent, Meta affirmatively promises users that it requires "Partners" to have the right to share the users' data before providing it to Meta.

95. Before April 2018, Meta's contract did not require Partners to have the lawful right to share user data before doing so:

Before April 19, 2018

Information from websites and apps that use our Services.
We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us.

Information from third-party partners.
We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.

After April 19, 2018

Information from partners.
Advertisers, app developers, and publishers can send us information through Meta Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities off of our Products—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services —whether or not you have an account or are logged into our Products. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third party data providers who have the rights to provide us with your information.

Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. Learn more about the types of partners we receive data from.

To learn more about how we use cookies in connection with Meta Business Tools, review the Facebook Cookies Policy and Instagram Cookies Policy.

96. Meta changed this provision again in July 2022 to remove the word "lawful" while still promising that it requires partners to have the right to share patient information with Meta:[23]

97. Meta does not verify that healthcare providers or covered entities have provided adequate notice and obtained valid consent or authorization to share their patients' data with Meta.[24]

> **How do we collect or receive this information from partners?**
>
> Partners use our Business Tools, integrations and Meta Audience Network technologies to share information with us.
>
> These Partners collect your information when you visit their site or app or use their services, or through other businesses or organizations they work with. We require Partners to have the right to collect, use and share your information before giving it to us.

98. Meta's contract with healthcare providers for use of the Meta Pixel does not mention HIPAA.

99. Meta does not use an advanced technical system to monitor whether Meta Collection Tools are installed on websites that will transmit individually identifiable health information to Meta. To the contrary, Meta Health urges healthcare providers and other covered entities to use Meta Collection Tools to target ads to patients.

---

[23] Meta, *Data Policy: Information from Partners, vendors and third parties* (Jan. 1, 2023), *https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartners Vendors.*

[24] The European Union recently ruled that Meta's attempt to obtain consent from users by including a clause in its terms and conditions allowing Meta to collect their data for personal advertising violated Europe's General Data Protection Regulation. Adam Satariano, *Meta's Ad Practices Ruled Illegal Under E.U. Law*, N.Y. Times (Jan. 4, 2023), *https://www.nytimes.com/2023/01/04/technology/meta-facebook-eu-gdpr.html.*

100. Meta maintains a "Health" marketing division called Meta Health, with a page at *https://www.facebook.com/business/industries/consumer-goods/healthcare* where Meta offers advertisers the chance to "get help growing your healthcare business" and explains how "Healthcare marketers are partnering with Meta."

101. The underlying metadata written for this page by Meta describe the page keywords to include: "<meta name="keywords" content="healthcare, marketers, Facebook, meta for business, healthcare business, virtual healthcare, preventative healthcare" />."

102. Meta Health is dedicated to helping web developers and advertisers in healthcare related industries to increase their marketing spend with Meta and improve their marketing campaigns using Meta Collection Tools.

103. Meta Health's role is to "inform" healthcare marketers "to think about how we can really disrupt health and how we market to patients."[25]

104. Meta Health employees are assigned to specific healthcare providers and other covered entities to encourage and aid their use of Meta Collection Tools for targeting patients.

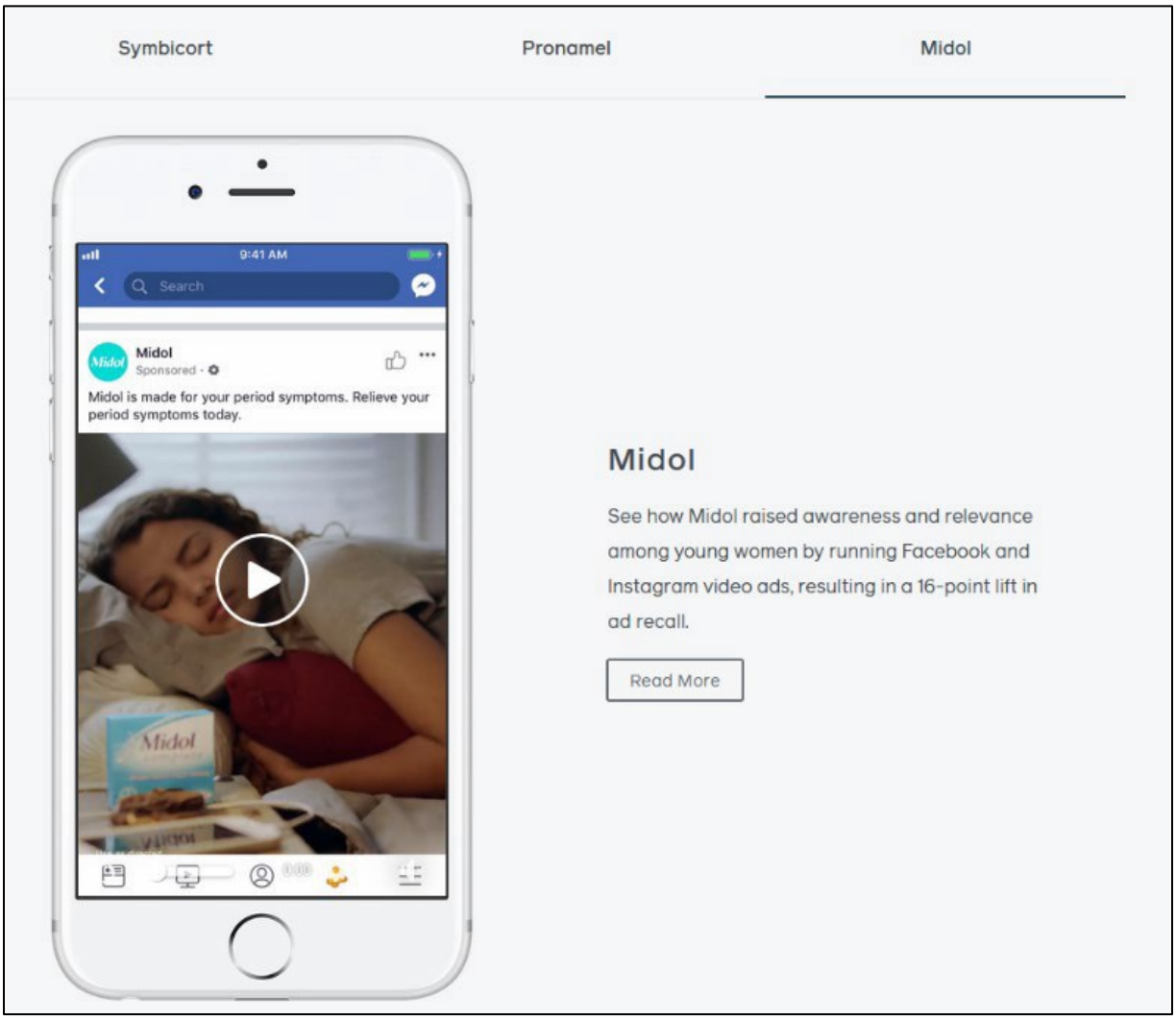
105. Meta provides guidance and resources for web developers and advertisers on a dedicated webpage at *https://www.facebook.com/business/industries/health*. Among other things, this webpage includes examples of advertising campaigns so that web developers and advertisers can "See how health brands are reaching new audiences with Facebook advertising."

106. The underlying metadata written for this page by Meta describes the page keywords to include: ""<meta name="keywords" content="Facebook for health, Facebook marketing for health communities, Facebook ad solutions for health brands, social media marketing, Facebook

[25] Facebook Disrupting Health: A Conversation with Jasson Gilmore, *https://www.facebook.com/business/industries/health?deeplink=829704181304626*.

video ads Facebook for mobile advertising, health campaign marketing, reach new patients online Facebook ads, advertising on Facebook" />."

107. For example, Meta highlights an advertising campaign aimed at "young women" through video ads promising to "Relieve your period symptoms today." [26]



[26] *Midol* (2023), *https://www.facebook.com/business/success/2-midol.*

108. Meta has also engaged in similar advertising campaigns relating to treatments for acne, allergies, arthritis, birth control, diabetes, erectile dysfunction, hair loss, high cholesterol, migraines, and many more prescription drugs and treatments.[27]

DEFENDANT'S CONDUCT VIOLATES FEDERAL AND STATE PRIVACY LAWS

The HIPPA Privacy Rule Protects Patient *Healthcare* Information

109. Patient healthcare information in the United States is protected by federal law under HIPAA and its implementing regulations, which are promulgated by the HHS.

110. The HIPAA Privacy Rule, located at 45 C.F.R. § 160 and 45 C.F.R. § 164 (A) and (E): "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically.[28]

111. The Privacy Rule broadly defines "protected health information" ("PHI") as "individually identifiable health information" ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

112. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual;

---

[27] *See generally* Meta, Get winning advertising solutions from businesses like yours (2023), *https://www.facebook.com/business/success/categories/health-pharmaceuticals.* The "marketing case studies" on this page change on occasion.

[28] HHS.gov, *Health Information Privacy* (Mar. 31, 2022), *https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.*

or the past, present, or future payment for the provision of healthcare to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

113. Under the HIPAA de-identification rule, "health information is not individually-identifiable only if: (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

a. Names;

b. Medical record numbers;

c. Account numbers;

d. Device identifiers and serial numbers;

e. Web Universal Resource Locators (URLs);

f. Internet Protocol (IP) address numbers; … and

g. Any other unique identifying number, characteristic, or code…; and" the covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is subject of the information." 45 C.F.R. § 164.514.

114. The HIPAA Privacy Rule requires any "covered entity"—which includes healthcare providers like UCMC—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

115. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually-identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually-identifiable health information … if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320(d)(6).

116. The criminal and civil penalties imposed by 42 U.S.C. § 1320(d)(6) apply directly to Meta when it is knowingly obtaining individually-identifiable health information relating to an individual, as those terms are defined under HIPAA.

117. Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties where "the offense is committed with intent to sell, transfer, or use individually-identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320(d)(6)(b). In such cases, an entity that knowingly obtains individually-identifiable health information relating to an individual "shall be fined not more than $250,000, imprisoned not more than 10 years, or both." 42 U.S.C. § 1320(d)(6)(b)(1).

HIPAA Protects Patient *Status* Information

118. HIPAA also protects against revealing an individual's status as a patient of a healthcare provider.

119. Guidance from HHS confirms that HIPAA protects patient status:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data.… **If such information was listed with health condition, healthcare provision or payment data, such as an indication that an individual was treated at a certain clinic, then this**

information would be PHI.[29]

120. HHS's guidance for marketing communications states that healthcare providers may not provide patient lists for marketing purposes without the consent of every included patient:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, **covered entities may not sell lists of patients to third parties without obtaining** authorization from each person on the list.[30]

121. HHS has previously instructed that the HIPAA privacy Rule protects patient status:

a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002);

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013); and

d. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even

---

[29] Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* at 5 (emphasis added) (Nov. 26, 2012), *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De- identification/hhs_deid_guidance.pdf.*

[30] Office for Civil Rights, *Marketing* at 1-2 (emphasis added) (Apr. 3, 2003), *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.*

> then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

HIPAA's Protections Do Not Exclude Internet Marketing

122. In December 2022, HHS issued a bulletin "to highlight the obligations" of healthcare providers and their business associates under the HIPAA Privacy Rule "when using online tracking technologies" such as the "Meta Pixel," which "collect and analyze information about how internet users are interacting with a regulated entity's website or mobile application."[31]

123. In this bulletin, HHS confirmed that HIPAA applies to healthcare providers' use of tracking technologies like the Meta Pixel.[32] Among other things, HHS explained that healthcare providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information (like an IP address) even if no treatment information is included and even if the individual does not have a relationship with the healthcare provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
>
> Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website or mobile app, including individually-identifiable health information (IIHI) that the individual providers when they use regulated entities' websites or mobile apps. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the

[31] HHS.gov, *HHS Office of Civil Rights Issue Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information* (Dec. 1, 2022), *https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html.*

[32] HHS.gov, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.*

> regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of healthcare services. **This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.* it is indicative that the individual has received or will receive healthcare services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or healthcare or payment for care**.

124. HHS explained that tracking technologies on healthcare providers' patient portals "generally have access to PHI" and may access diagnosis and treatment information, in addition to other sensitive data:

> Tracking on user-authenticated webpages
>
> Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. **Tracking technologies on a regulated entity's user-authenticate webpages generally have access to PHI.** Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. **Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal**. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to **only** use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.

125. HIPAA applies to healthcare providers' webpages with tracking technologies even outside the patient portal:

> Tracking on unauthenticated webpages
>
> [T]racking technologies on unauthenticated webpages may access to PHI, in which case the HIPAA Rules apply to the regulated

> entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal … **[and pages] that address[] specific symptoms or health conditions,** such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering **credentials may have access to PHI in certain circumstances**. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a healthcare provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.

126. As a result, a healthcare provider may not disclose PHI to a tracking technology vendor, like Meta, unless it has properly notified its website users and entered into a business associate agreement with the vendor:

> Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use. However, the Privacy Rule does **not** permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI. If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individual's HIPAA-compliant authorizations are required **before** the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do **not** constitute a valid HIPAA authorization. [I]t is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.

127. HHS's bulletin did not create any new obligations. Instead, it merely highlighted long-standing obligations based on previous guidance and rules that have been in place for decades.

The FTC Act Protects Health Information

128. In the context of this case, the FTC has made clear that "health information" is "anything that conveys information—or enables an information—about a consumer's health" and provides an example that location-data alone (such as repeated trips to a cancer treatment facility") "may convey highly sensitive information about a consumer's health." Jillson, Elisa, *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, Federal Trade Commission (July 25, 2023), *https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases*. The FTC has joined HHS in notifying HIPAA-covered entities and non-HIPAA-covered entities that sharing such "health information" with Google and Facebook is an unfair business practice under federal law:

> When consumers visit a hospital's website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."[33]

[33] *FTC and HHS Warn Hospital Systems and Telehealth Providers About Privacy and Security Risks from Online Tracking Technologies*, Federal Trade Commission (July 20, 2023), *https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking*.

Illinois Law Protects Health Information

129. For example, 410 ILCS 50/3(d) provides that: "Each physician, health care provider, health services corporation and insurance company shall refrain from disclosing the nature or details of services provided to patients."

130. Thus, Illinois law requires all hospitals, including UCMC, to maintain all medical records and information within their control as confidential, rendering UCMC's actions with respect to the interception and disclosure of its patients' health communications to Meta unlawful under Pennsylvania law.

Patients Have Protectable Property Interests In Their Individually-Identifiable Health Information

131. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things like data and communications. Plaintiff and the Class members have a vested property right in their individually-identifiable health information.

132. Courts have described the concept of "property" broadly:

a. "'Property' has been defined to include every interest anyone may have in any and everything that is the subject of ownership by man, together with the right to freely possess, use, enjoy or dispose of the same; and this right of user [is] a part of the property right guaranteed by the constitutions." *See Father Basil's Lodge, Inc. v. Chicago*, 393 Ill. 246, 256 (1946).

b. "In its broadest and most inclusive sense 'property' subsumes all rights and interests in real and personal holdings." *See Davis v. Attic Club*, 56 Ill. App. 3d 58, 66 (1977).

c. "In Illinois, the term 'property' has been defined as 'a word of the very broadest import, connoting any tangible or intangible res which might be made the subject of ownership.'" *See In re Marriage of Hunt*, 78 Ill. App. 3d 653, 662 (1979), *quoting Harvey Wrecking Co. v. Certain Underwriters at Lloyd's, London* 91 Ill. App. 2d 449, 455-56 (1968).

133. Federal and state law grant patients the right to protect the confidentiality of data that identifies them as patients of a particular healthcare provider and restrict the use of their health data, including their status as a patient, to only uses related to their care or otherwise authorized by federal or state law in the absence of patient authorization.

134. A patient's right to protect the confidentiality of their health data and restrict access to this data is valuable.

135. In addition, patients enjoy property rights in the privacy of their health communications under statutes such as HIPAA; and 410 ILCS 50/3(d). State health privacy laws and American courts have long recognized common law property rights in the content of a person's communications that are not to be used or disclosed to others without authorization.

136. Property rights in communications and information privacy are established by:

d. The Electronic Communications Privacy Act, including Title I (the Wiretap Act); Title II (the Stored Communications Act); and Title III (the Pen Register Act);

e. State laws, including 410 ILCS 50/3(d); and

f. Common law information property rights regarding the exclusive use of confidential information that have existed for centuries and continue to exist, s*ee Folsom v. Marsh*, 9 F.Cas. 342, 346 (C.C.D. Mass. 1841) (Story, J); *Baker v. Libbie*, 210 Mass. 599, 602 (1912); *Denis v. LeClerc*, 1 Mart. (La.) 297 (1811).

137. Meta's CEO Mark Zuckerberg has expressly acknowledged that Meta users have an ownership interest in their data. In 2010, when Meta first revealed its "Download Your Information" tool, Zuckerberg stated that, "People own and have control over all info they put into Facebook and 'Download Your Information' enables people to take stuff with them."[34] Although

[34] *https://techcrunch.com/2010/10/06/facebook-now-allows-you-to-download-your-information/.*

Zuckerberg's statements regarding people's ability to "control" the information "put into Facebook" and the ability to access all such data via DYI is not true, his statement about data ownership is true.

138. UCMC's unauthorized interception and disclosure of Plaintiff's and the Class members' individually identifiable health information violated their property rights to control how their data and communications are used and who may be the beneficiaries of their data and communications.

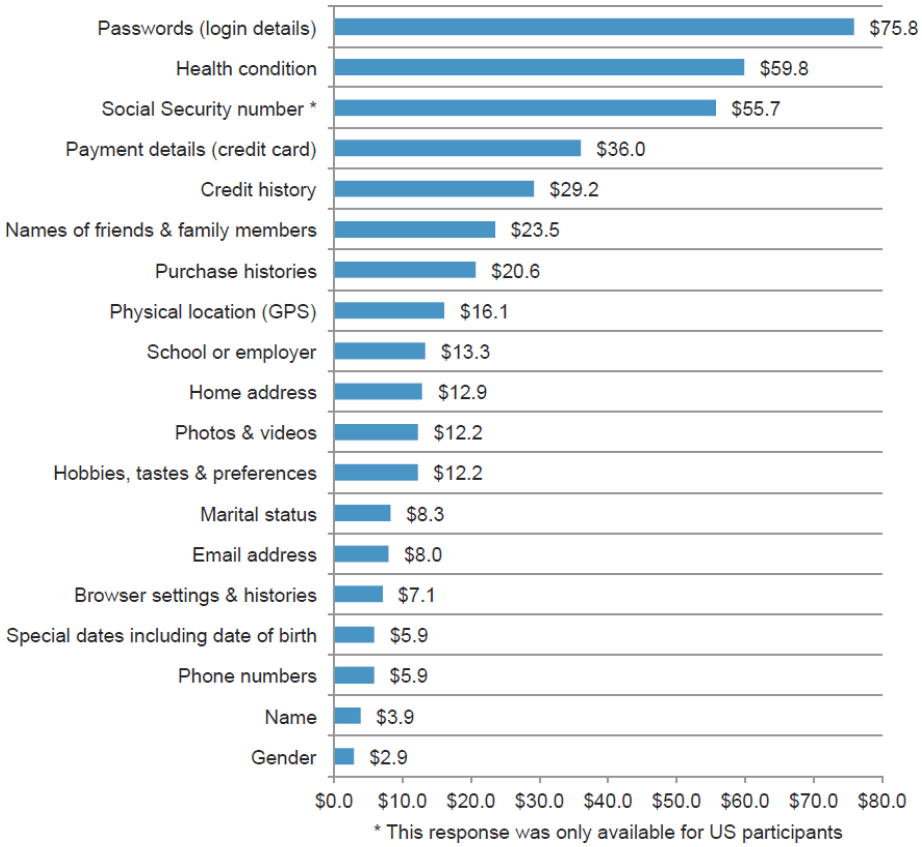
The Information UCMC Intercepts And Discloses To Meta Without Plaintiff's Or Class Members' Consent Has Actual, Measurable Monetary Value

139. Meta "generate[s] substantially all of [its] revenue from advertising."[35]

140. Meta annually receives billions of dollars of unearned advertising sales revenue from Meta healthcare Partners, including UCMC, who are targeting Facebook users based on their health information.

141. The data that Meta collects without authorization has monetary value. For example, a 2015 study found respondents placed a value of $59.80 on an individual's health information:

[35] Meta 2022 Annual Report at 17.



THE PARTIES

142. UCMC is an Illinois not-for-profit corporation headquartered in Chicago, Illinois. UCMC encourages patients, which number in the thousands, to use and communicate with medical providers through its Website. The Pritzker School of Medicine, Biological Sciences Division, Medical Center, Community Health and Hospital Division, and UChicago Medicine Physicians are all a part of UCMC. UCMC encourages its patients, which number in the thousands, to use and communicate with their medical providers through UCMC's Website.

143. Sophia Hartley is a natural person and a citizen of the State of Wisconsin. Plaintiff has been a patient of UCMC since at least 2018. Plaintiff has also been a *www.uchicagomedicine.org* user since at least 2018. During the relevant time period, Plaintiff has used the UCMC Website to schedule appointments, request information on specific medical

services, and research providers. By doing so, Plaintiff's individually identifiable health information was disclosed to Meta under the systematic process described herein. Plaintiff had no knowledge her sensitive medical information was shared with Meta or other third parties and gave no consent or authorization for UCMC to disclose her individually identifiable health information.

144. During the relevant time period, when Meta Collection Tools were present, Plaintiff used UCMC's public website, *www.uchicagomedicine.org*, to search for a primary care physician. The full scope of UCMC's interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery. However, UCMC intercepted at least the following communications about Plaintiff's prospective healthcare providers. The following long-URLs or substantially similar URLs were sent to Meta via Meta's Collection Tools:

- https://www.uchicagomedicine.org/find-a-physician
- https://mychart.uchospitals.edu/mychart/

145. Contemporaneously with the interception and transmission of Plaintiff's communications on *www.uchicagomedicine.org*, UCMC also disclosed to Meta Plaintiff's personal identifiers, including but not limited to her IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers.

146. When Plaintiff engaged in these communications with UCMC's Website, Meta's Collection Tools intercepted individually identifiable health information that included: her status as a UCMC patient, the dates and times she logged-in to the MyChart, and the webpages she clicked and viewed related to her medical providers, conditions, and treatments. Because UCMC's and Meta's conduct was surreptitious and conducted through back-end electronic systems and processes, Plaintiff will seek specific information about these intercepted and transmitted communications in discovery. However, when Plaintiff used her computer to access UCMC's Website and log-in to the UCMC MyChart patient portals, which she did many times during the

relevant period, the Meta Collection Tools on UCMC's Website sent at least the following personally identifiable patient information and patient health information to Meta[36]:

a. Hartley was communicating with UCMC on its *www.uchicagomedicine.org* website and its MyChart patient portal (*https://mychart.uchospitals.edu/mychart.*);

b. Hartley engaged in an "ev,"' or event, called a SubscribedButtonClick, or something substantially similar;

c. Descriptive URLs that describe the categories of the website, categories that describe the current section of the website, and the referrer URL that caused navigation to the current page;

d. The content of the button Hartley clicked was "Sign In" to MyChart, or something substantially similar;

e. The page on which Hartley clicked the button was "Patient Portal," "Home," or something substantially similar;

f. Hartley had previously visited a UCMC page;

g. Hartley's Internet Protocol address;

h. Identifiers that Facebook uses to identify Hartley and her device, including but not limited to, the "c-user," "datr," "fr," and "fbp cookies;" and

i. Browser attribute information sufficient to fingerprint. Hartley's device.

147. As a result, the Meta Pixel and Collection Tools on UCMC's Website intercepted and disclosed to Meta information about Hartley's identity, her log-in to the patient portal, the and the content of the communications she made on UCMC's Website.

[36] Plaintiff's investigation has revealed that UCMC has removed the Meta Collection Tools from its Website. Accordingly, the full extent of UCMC's interception and disclosure of individually-identifiable health information can only be determined through formal discovery.

148. UCMC never notified Hartley that either it or Meta would put individually identifiable patient health information about her past, present, or future health conditions to their own commercial uses. Hartley never provided informed consent or written permission allowing UCMC to send individually identifiable patient health information about her past, present, or future health conditions to Meta. Hartley never provided informed consent or written permission allowing UCMC or Meta to put individually identifiable patient health information about her past, present, or future health conditions to their own commercial use.

149. Meta used the intercepted content of Hartley's communication with UCMC to repeatedly serve her ads "focused" on her status as a patient of UCMC and the specific actions she performed on UCMC's Website, including but not limited to:

a. The telehealth platform "Hers" (for mental health treatment)

150. Meta maintains a history of every ad it has shown to Plaintiff and the Class members, both on and off Meta's social media sites, including on Meta properties and the Facebook Audience Network through which Meta serves ads to Facebook users on non-Meta websites. Plaintiff intends to seek this information in discovery to fully inform the scope of her claims and damages.

CLASS ACTION ALLEGATIONS

151. Plaintiff brings this action as a class action under Federal Rules of Civil Procedure 23(a) and (b)(3) for:

> All persons whose protected health information was disclosed to Meta without authorization or consent through the Meta Collection Tools on UCMC's Website until August 30, 2022.

("the Class members").

152. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(1), because the Class members are so numerous and geographically dispersed that their joinder would be impracticable. Plaintiff believes that Defendant's and Meta's business records will permit the identification of thousands of people meeting the Class definition.

153. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(2), because there are many common questions of facts and law concerning and affecting the Class members, including:

g. Whether UCMC had a duty to protect and refrain from disclosing the Class members' individually identifiable health information;

h. Whether UCMC intentionally disclosed the Class members' individually identifiable health information to Meta;

i. Whether the Class members consented to UCMC's disclosure of their individually identifiable health information to Meta;

j. Whether the Class members are entitled to damages because of UCMC's conduct; and

k. Whether UCMC's knowing disclosure of its patients' individually identifiable health information to Meta is "criminal or tortious" under 18 U.S.C. § 2511(2)(d).

154. Plaintiff also anticipates that Defendant will raise defenses common to the Class.

155. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(3), because Plaintiff's claims are typical of the claims belonging to the Class members. Plaintiff and the Class members were harmed by the same wrongful conduct perpetrated by Defendant that caused their individually identifiable health information to be intercepted and disclosed without notice or consent. As a result, Plaintiff's claims are based on the same facts and legal theories as the Class members' claims.

156. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(4), because Plaintiff will fairly and adequately protect the interests of all the Class members, there are no known conflicts of interest between Plaintiff and the Class members, and Plaintiff has retained counsel experienced in the prosecution of complex litigation.

157. Class certification is appropriate under Fed. R. Civ. P. 23(b)(3), because common questions of law and fact predominate over questions affecting the individual Class members, because a class action is superior to other available methods for the fair and efficient adjudication of these claims and because important public interests will be served by addressing the matter as a class action. Further, the prosecution of separate actions by the individual Class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendant and substantially impair the Class members' ability to protect their interests.

TOLLING

158. Any statute of limitations applicable to Plaintiff's claims has been tolled by UCMC's actual knowledge and efforts to conceal the misrepresentations and omissions alleged herein. Through no fault or lack of diligence, Plaintiff and the Class members had no obvious way to discover UCMC's deception and unlawful conduct.

159. Plaintiff and the Class members did not discover and did not know of any facts that would have caused a reasonable person to suspect that UCMC was acting unlawfully. The earliest Plaintiff or a reasonable user of UCMC's Website could have learned about UCMC's conduct was approximately June of 2022 when an investigative report revealed that UCMC had installed the Pixel onto its Website and was disclosing sensitive health information to Meta.[37] UCMC's alleged

[37] *See*, Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook is Receiving Sensitive Medical Information from Hospital Websites,* THE MARKUP (June 16, 2022), available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited December 3, 2024).

representations were material to Plaintiff and the Class members at all relevant times. During any applicable statute of limitations, Plaintiff and the Class members could not have discovered UCMC's alleged wrongful conduct through the exercise of reasonable diligence because UCMC's incorporation of the Pixels is highly technical, undiscoverable by ordinary users of UCMC's Website, and UCMC made no disclosures or other indications that would inform a reasonable user of its Website that UCMC was intercepting and disclosing users' individually-identifiable health information to Meta.

160. At all relevant times, UCMC was – and still is – under a continuous duty to disclose to Plaintiff and the Class members the true nature of the disclosures being made and the lack of an actual "requirement" before it shared Plaintiff's and the Class members' data with Meta.

161. UCMC's knowingly, actively, affirmatively, or negligently concealed the facts alleged herein. Plaintiff and the Class members reasonably relied on UCMC's concealment.

162. For these reasons, all applicable statutes of limitation have been tolled based on the discovery rule and UCMC's concealment, and UCMC is estopped from relying on any statutes of limitations in defense of this action.

COUNT I
Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.*

163. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

164. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

165. The ECPA protects both the sending and receipt of communications.

166. The ECPA provides a private right of action to any person whose electronic communications are intercepted. 18 U.S.C. § 2520(a).

167. UCMC intentionally intercepted electronic communications that Plaintiff and the Class members exchanged with UCMC through the Meta Collection Tools installed on the UCMC's Website.

168. The transmissions of data between Plaintiff and the Class members and UCMC qualify as communications under the ECPA. 18 U.S.C. § 2510(12).

169. UCMC contemporaneously intercepted and transmitted Plaintiff's and the Class members' communications to Meta.

170. The intercepted communications include:

l. the content of Plaintiff's and the Class members' registrations for patient portals, including clicks on buttons to "Register" or "Signup" for portals;

m. the content Plaintiff's and the Class members' log in and log out of patient portals, including clicks to "Sign-in," "Log-in," "Sign-out," or "Log-out";

n. the content of communications that Plaintiff and the Class members exchange inside patient portals immediately before logging out of the portals;

o. the content of Plaintiff's and the Class members' communications relating to appointments with medical providers;

p. the content of Plaintiff's and the Class members' communications relating to specific healthcare providers, conditions, treatments, diagnoses, prognoses, prescription drugs, symptoms, insurance, and payment information; and

q. Full-string URLs that contain any information concerning the substance, purport, or meaning of patient communications with their health entities.

171. For example, Defendant's interception of the fact that a patient views a webpage like *https://www.uchicagomedicine.org/cancer/types-*

treatments/breast-cancer involves "content," because it communicates that patient's request for the information on that page.

172. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. the cookies UCMC and Meta use to track Plaintiff's and the Class members' communications;

b. Plaintiff's and the Class members' browsers;

c. Plaintiff's and the Class members' computing devices;

d. UCMC's web-servers or webpages where the Meta Collection Tools are present;

e. Meta's web-servers; and

f. the Meta Collection Tools source code UCMC deploys on its Website to acquire Plaintiff's and the Class members' communications.

173. Meta is not a party to Plaintiff's and the Class members' communications with UCMC.

174. UCMC transmits the content of Plaintiff's and the Class members' communications to Meta through the surreptitious redirection of those communications from Plaintiff's and the Class members' computing devices.

175. Plaintiff and the Class members did not consent to Meta's acquisition of their appointment, and treatment communications with UCMC.

176. Meta did not obtain legal authorization to obtain Plaintiff's and the Class members' communications with UCMC relating to communications with their health entities.

177. Meta did not require UCMC to obtain the lawful rights to share the content of Plaintiff's and the Class members' communications relating to patient portals, appointments, and treatments.

178. Any purported consent that Meta received from UCMC to obtain the content of Plaintiff's and the Class members' communications was not valid.

179. In disclosing the content of Plaintiff's and the Class members' communications relating to, treatments, conditions, and appointments, UCMC had a purpose that was tortious, criminal, and designed to violate state constitutional and statutory provisions including:

a. the unauthorized disclosure of individually identifiable health information is tortuous in and of itself regardless of whether the means deployed to disclose the information violates the Wiretap Act or any subsequent purpose or use for the acquisition. UCMC intentionally committed a tortious act by disclosing individually identifiable health information without authorization to do so.

b. the unauthorized acquisition of individually identifiable health information is a criminal violation of 42 U.S.C. § 1320d-6 regardless of any subsequent purpose or use of the individually identifiable health information. UCMC intentionally violated 42 U.S.C. 1320d-6 by intentionally disclosing individually identifiable health information without authorization.

c. a violation of HIPAA, particularly 42 U.S.C. § 1320d-6, which is a criminal offensive punishable by fine or imprisonment with *increased penalties* where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage [or] personal gain." UCMC intentionally violated the enhanced penalty provision of 42 U.S.C. § 1320d-6 by disclosing the individually identifiable health information "with intent to sell transfer or use" it for "commercial advantage [or] personal gain."

d. a knowing intrusion upon Plaintiff's and the Class members' seclusion;

e. trespass upon Plaintiff's and the Class members' personal and private property via the placement of an _fbp cookie associated with UCMC's Website on Plaintiff's and the Class members' personal computing devices;

f. the requirement under 410 ILCS § 5/30 that healthcare providers maintain the confidentiality of patient health records; and

g. violation of the federal wire fraud statutes at 18 U.S.C. §§ 1343 (fraud by wire, radio, or television) and 1349 (attempt and conspiracy), which prohibit a person from "devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate … commerce, any writing, signs, signals, pictures, or sounds for purpose of executing such scheme or artifice."

180. The federal wire fraud statute, 18 U.S.C. § 1343, has four elements: (1) that the defendant voluntarily and intentionally devised a scheme to defraud another out of money or property; (2) that the defendant did so with the intent to defraud; (3) that is was reasonably foreseeable that interstate wire communications would be used; and (4) that interstate wire communications were in fact used. The attempt version of the wire fraud statute provides that "[a]ny person who attempts or conspires to commit any offense under this chapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy." 18 U.S.C. § 1349.

181. UCMC's scheme or artifice to defraud in this action consists of:

a. the false and misleading statements and omissions in its privacy policies set forth above, including the statements and omissions recited in the breach of contract and negligence claims below;

b. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie of UCMC's Website rather than a third-party cookie from Meta.

182. UCMC acted with the intent to defraud in that it willfully invaded and took Plaintiff's and the Class members' property:

a. property rights to the confidentiality of their individually identifiable health information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and

b. property rights to determine who has access to their computing devices.

183. UCMC acted with the intent to defraud in that it willfully invaded and took Plaintiff's and the Class members' property:

a. with knowledge that (1) UCMC did not have the right to share such data without written authorization; (2) courts had determined that a healthcare providers' use of the Meta Pixel gave rise to claims for invasion of privacy and violations of state criminal statutes; (3) a reasonable Facebook user would not understand that Meta was collecting their individually-identifiable health information based on their activities on UCMC's Website; (4) a reasonable Facebook user would be shocked to realize the extent of Meta's collection of individually-identifiable health information; (5) a Covered Incident had occurred which required a report to be made to the FTC pursuant to Meta's consent decrees with the FTC; and (6) the subsequent use of health information for advertising was a further invasion of such property rights in making their own exclusive use of their individually-identifiable health information for any purpose not related to the provision of their healthcare; and

b. with the intent to (1) acquire Plaintiff and the Class members' individually-identifiable health information without their authorization and without their healthcare providers or covered entities obtaining the right to share such information; (2) use Plaintiff's and the Class members' individually-identifiable health information without their authorization; and (3) gain access to the Plaintiff's and the Class members' personal computing devices through the 'fbp' cookie disguised as a first-party cookie.

184. Any purported consent provided by UCMC using the Meta Collection Tools had a purpose that was tortious, criminal, and in violation of state constitutional and statutory provisions because it constitutes:

a. knowing intrusion into a private matter that would be highly offensive to a reasonable person;

b. a violation of 42 U.S.C. § 1320d-6, which is a criminal offense punishable by fine or imprisonment and that includes increased penalties where "the offense is committed with intent to sell, transfer, or use individually-identifiable health information for commercial advantage [or] personal gain."

c. trespass;

d. breach of fiduciary duty; and

e. a violation of various state health privacy and computer privacy statutes, including the CCPA.

185. Plaintiff and the Class members have suffered damages because of UCMC's violations of the ECPA that include:

a. UCMC eroded the essential, confidential nature of the provider-patient relationship;

b. UCMC failed to provide Plaintiff and the Class members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information;

c. UCMC derived valuable benefits from using and sharing the contents of Plaintiff's and the Class members' communications on its Website without their knowledge or informed consent, and without providing any compensation for the information it used or shared;

d. UCMC's actions deprived Plaintiff and the Class members of the value of their individually identifiable health information;

e. UCMC's actions diminished the value of Plaintiff's and the Class Members' property rights in their individually identifiable health information; and

f. violating Plaintiff's and the Class members' privacy rights by sharing their individually identifiable health information for commercial use.

186. For UCMC's violations set forth above, Plaintiff and the Class members seek appropriate equitable or declaratory relief, including injunctive relief; actual damages and "any

profits made by [UCMC] as a result" of its violations or the appropriate statutory measure of damages; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred pursuant to 18 U.S.C § 2520.

187. Unless enjoined, UCMC will continue to commit the violations of law alleged here.

188. Plaintiff wants to continue to communicate with their healthcare provider through online platforms but have no practical way of knowing if their communications are being intercepted and disclosed to Meta, and thus continue to be at risk of harm from UCMC's conduct.

189. Pursuant to 18 U.S.C. § 2520, Plaintiff and the Class members seek monetary damages for the *greater of* (i) the sum of the actual damages suffered by the plaintiff and any profits made by UCMC as a result of the violation or (ii) statutory damages of whichever is greater of $100 a day for each violation or $10,000.

PRAYER FOR RELIEF

Wherefore, Plaintiff respectfully asks this Court for an Order:

a. certifying this case as a class action, appointing Plaintiff as Class Representative, and appointing Stephan Zouras LLP as Class Counsel;

b. entering judgment for Plaintiff and the Class members on their ECPA claim and awarding all damages available under 18 U.S.C. § 2520, including equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs;

c. awarding injunctive relief to Plaintiff and the Class members that includes an order barring Defendant from any further interception, transmission, or commercial use of Plaintiff's and the Class members' communications with their doctors and medical office staff on UCMC's Website absent express notice and informed consent;

d. awarding pre- and post-judgment interest on all damages awarded;

e. awarding recovery of Plaintiff's reasonable attorneys' fees and reimbursement of their litigation expenses; and

f. awarding such additional relief as justice requires.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Respectfully Submitted,

Dated: April 11, 2025

/s/ *James B. Zouras*

Ryan F. Stephan
James B. Zouras
Teresa M. Becvar
Michael J. Casas
STEPHAN ZOURAS, LLP
222 W. Adams Street, Suite 2020
Chicago, Illinois 60606
312.233.1550
312.233.1560 f
rstephan@stephanzouras.com
jzouras@stephanzouras.com
tbecvar@stephanzouras.com
mcasas@stephanzouras.com

ATTORNEYS FOR PLAINTIFF

CERTIFICATE OF SERVICE

I, Michael J. Casas, an attorney, hereby certify that I caused the foregoing **THIRD AMENDED CLASS ACTION COMPLAINT** to be filed with the Court using the ECF/CM system, which will send notice and copy of such filing to all attorneys of record.

/s/ Michael J. Casas